웹 퍼블리싱 취약점 및 마크업 체크리스트

프로젝트명	웹 서비스 마크업 개발 전체 해당		
최초작성일	2024-06-29	수정일	07-02
점검일자			
점검자	전체		
점검 단계	dev		
FE 측 기술 버전	- jQuery 3.7.1 (최신 버전 항상 확인) - jQuery UI 1.13.3 2024-05-20 (최신 버전 항상 확인) - Vue.js 3.4.31 (2024-06-29 기준) - Vue.js 2.6.11 NES 또는 Vue.js 2.7.14 NES (HeroDevs https://www.herodevs.com/) [Reserved] - Axios 최신버전 항상 판단		
서버측 기술 버전	- Node.js 20.11.1 LTS (버전업이 필요한지 정기 판단) - Express.js 4.19.2 (버전업 필요한지 정기 판단, 5.x 베타버전이 정식 버전으로 바뀌는지 확인)		

취약점 분류 1			
항목	세부 항목	점검 내용	점검 결과
자동화도구	소나린트 (SonarLint)	소나린트 자동화도구로 소스코드를 점검하고 경고 및 에러를 수정하였는가?	항상 확인
XSS 출력 데이터 인코딩	〈, 〉 문자 인코딩	<, > 로 변환하여 스크립트 실행 방지	협의
XSS 출력 데이터 인코딩	HTML 인코딩, URL 인코딩	HTML 본문에 출력되는 문자열은 HTML 인코딩을 하고, URL 파라미터로 쓰이는 부분은 URL 인코딩을 한다.	
XSS 출력 데이터 인코딩	템플릿 엔진 변수 활용	템플릿 엔진 변수는 출력시 자동으로 HTML 인코딩을 적용하여 HTML 인젝션 방지	
입력값 검증	데이터형 판단	Number형, Object형 판단	
입력값 검증	파일업로드	HTML5 어트리뷰트 accept, required, multiple을 활용	
클릭재킹		투명한 div 등을 화면 위에 레이어로 겹쳐 사용자를 속이는 행위. 사용자가 보이지 않는 버튼을 클릭하게 유도함. CSS 속성 position:absolute;opacity:0;로 간단히 재현 가능	점검
폼 태그	input	input 요소 입력 길이 제한	협의
폼 태그	hidden field	히든 필드를 사용할 경우 서버에서 반드시 검증	

폼 태그	input	숫자 입력의 경우 자바스크립트로 유효성 검증 - 숫자 타입인지 확인 - 로직 작성	필수
취약점 분류 2			
에러 처리	필요시 항상	try - catch문이 필요한지 여부	
보안 헤더	X-Powered-By 헤더	서버 기반 라이브러리 이름 등 문자열 출력 제한여부	필수
보안 헤더	개행 문자 삭제	헤더 값 내 개행 문자 삭제 여부	해당없음
보안 헤더	클릭재킹 방어	Frame-busting 스크립트, X-Frame-Options 헤더 설정 등	해당없음
보안 헤더	CSP, Content Security Policy	웹페이지에서 로드 가능한 리소스 출처를 제한하여 XSS 공격 방어	
보안 헤더	HSTS	HTTPS 강제, HTTP--)HTTPS 리디렉션	
인스턴스 관리	OS 업데이트	최신 업데이트 여부	해당없음
인스턴스 관리	디스크 사용량	안전 상한선 체크, 메모리 스왑 정상 여부	해당없음

웹 퍼블리싱 점검표

마크업 체크리스트 분류			
항목	세부 항목	점검 내용	점검 결과
테이블(표)	width	각 셀별 width를 고정값으로 하는가?	예/아니오
체크박스 UI	Width	가로로 찌그러지는가?	
타이틀 바	장식	80% 불투명도 등이 적용되었는가?	
팝업 UI	본문 폰트	적용 여부	
검색바 UI	폰트 및 아이콘	아이콘과 폰트가 시안대로 반영되었는가?	
타이틀 바	문법	nav 태그를 사용할 것인지? (아니라면 LNB, RNB, MNB 세부 nav바를 적용)	예/아니오
a 태그	href	링크 데스티네이션이 명확한가?	
간격	gap	박스와 박스 사이 간격을 늘려야 하는가?	
아이콘 장식	i 태그	상세페이지 내 장식 아이콘이 빠져있지 않은가?	
Cursor	hand 모양 커서	링크 호버시 cursor: pointer; 적용 여부	
아코디언 UI	아이콘	업, 다운 아이콘이 표시되는가?	
아코디언 UI	글꼴 크기	글꼴 크기가 정확한가?	
아코디언 UI	애니메이션	패딩, 마진 CSS 수정으로 각 아이템의 height 값 증가로 애니메이션이 부자연스러운 경우: 애니메이션을 없앨 수 있는가?	
버튼	버튼화	현재 기능상 버튼이 아닌 HTML 요소들 중 버튼으로 만들어야 하는 것들이 있는가?	
페이지네이션	Prev 버튼	버튼 기능이 정상적으로 작동하는가?	필요시
페이지네이션	페이지 번호 리스트	유효한 페이지 번호만 출력되는가? 예를 들어 11...20 대신 11, 12로만	필요시
jQuery	객체 length	제이쿼리 객체 사용 전 length 체크 여부	예/아니오
Javascript	에러	“pagination is not defined” 커스텀 에러 정의 여부	
Javascript	에러	공통 에러 체크 함수 생성 여부	

저작권자 ⓒ 2017-2024 매니스탈링스, 파일 원본 사용, 2차 저작 가능, 상업적 무료 사용 허용
PDF 임베팅 폰트 : 한컴산뜻돋움 (저작권자 한컴)